

Amendments to the Specification

On page 2, after line 22, please add the following:

BRIEF DESCRIPTION OF THE DRAWINGS

The figure is a flow diagram illustrating a securing method according to the invention.

On page 2, please replace the paragraph beginning on line 18, with the following paragraph:

According to the invention, the method for securing a computer system by logical confinement of data comprises separation of said data ~~per possessor~~ per possessor P1...Px...Pn and their encryption with a dedicated key; this separation and encryption process is performed by a procedure comprising the following ~~steps~~ steps (see figure):

- an allocation of ~~memory~~ memory MAUx performed by a ~~memory manager~~ memory manager MM on request from another component of the operating system which transmits to said ~~memory manager~~ memory manager MM, the ~~identity~~ identity Id of the ~~requester~~ requester Px. This requester will become the ~~possessor~~ possessor Px of the allocated ~~memory~~ memory MAUx. Transmission of the ~~identity~~ identity Id of the requester may be accomplished either by managing a current context, or by passing parameters to the functions of the memory manager;
- a check by the aforesaid memory manager of the whole of the ~~memory allocation~~ units memory allocation units MAU1-MAUn, each being associated with a ~~possessor~~ a possessor P1-Pn of the memory allocation unit. Each memory

allocation unit can only have one single possessor; nevertheless, several memory allocation units may have the same possessor;

- an encryption of the data of each possessor by means of a key associated with this possessor;
- optionally, a use of a secret associated with each possessor, by the memory manager. This secret may typically be provided to the memory manager by the operating system at the moment when the possessor is introduced into the system and upon each access to a memory allocation unit;
- optionally, a use of a key for each possessor by the memory manager. This key may for example be derived from a secret associated with the possessor and a so-called "master" key to which only the memory manager has access;
- a check of the ~~identity~~identity Id of the requester by the memory manager for each request to access a memory allocation unit; if this ~~identity~~identity Id is not identical with ~~that of that Idx~~ of the possessor of said memory allocation unit, then the access to the ~~memory allocation unit~~memory allocation unit MAU_x is refused by the memory manager;
- performing, by means of the memory manager, encryption (in the case of a write request) or decryption (in the case of a read request) of the relevant data with the key associated with the possessor, whereby this key may be re-calculated by the memory manager.